Kathryn N. Nester, Federal Public Defender (#13967)
Daphne A. Oberg, Assistant Federal Public Defender (#11161)
Robert K. Hunt, Assistant Federal Public Defender (#5722)
46 West Broadway, Suite 110
Salt Lake City, Utah 84101
Telephone: (801) 524-4010
Fax: (801) 524-4060
Attorneys for Claud R. Koerber

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. CLAUD R. KOERBER, *Defendant.*	**MOTION TO RETURN AND SUPPRESS DEFENDANT'S PRIVATE COMPUTER RECORDS (INCLUDING ALL QUICKBOOKS FILES) OBTAINED BY THE GOVERNMENT THROUGH WARRENTLESS SEARCHES AND SEIZURES** *Oral Argument and Evidentiary Hearing Requested* Case No. 2:17-CR-37 District Judge Frederic Block

Undersigned counsel for Mr. Koerber recently learned that prosecutors and federal agents obtained a substantial portion of the core evidence presented by the government at the prior trial, and the bulk of the financial data used by government summary witnesses, via warrantless searches and seizures of electronic computer hard-drives and discs and by obtaining confidential passwords to Mr. Koerber's private and confidential records from employees not authorized to share said passwords. The government obtained the passwords and searched the records after Mr. Koerber (through counsel) had expressly refused to consent to the government's search and seizure of these same electronic records. The evidence at issue includes but is not limited to: the entire contents of the computer disc previously described by one of the employees (*See* Day 6, Trial Transcript at 1043, 1044, Government Exhibits 19, 20, 22, 23, and 24) and the entire

contents of the disc recently referenced by the government in Doc. 411 at page 3. Significantly, these unauthorized searches also include all of the personal and company QuickBooks files and databases previously used by the government at trial, previously used and relied upon by the government's summary witnesses and now by designated experts Ms. Mennitt and Mr. Roberts.

Overview

The government's case against Mr. Koerber centers upon fraud allegations, and at the core of these allegations is the evidence of Mr. Koerber's personal and business financial activities. The most significant financial activities, according to the government, relate to specific financial transactions alleged to have taken place between November 4, 2005 (Counts 2 and 5) and September 21, 2007 (Count 14). As such, on June 21, 2018, the government recently produced its notice of an expert witness related to these financial activities, and also produced discovery and proposed exhibits related thereto. *See* Doc. 407. A significant portion of evidence that the government intends to introduce at the coming re-trial of Mr. Koerber, including the core financial evidence relied upon by the government's expert Ms. Mennet, derives from his private computer files (including password protected Quickbooks files) that the government obtained after Mr. Koerber (through counsel) expressly and repeatedly refused to voluntarily disclose or deliver such records to the government, and only by multiple, warrantless seizures and multiple subsequent warrantless searches of these electronic files by federal government agents.

Legal Standard

Under local rule DUCrimR 12-1(e), a motion to suppress which also requests an evidentiary hearing, "shall state with particularity and in summary form without an accompanying legal brief the following: (i) the basis for standing; (ii) the evidence for which suppression is sought; and (iii) a list of the issues raised as grounds for the motion." The rule also

provides that, "[u]nless the court otherwise orders, ***neither a memorandum of authorities nor a response by the government is required.*** At the conclusion of the evidentiary hearing, the court will provide reasonable time for all parties to respond to the issues of fact and law raised in the motion unless the court has directed pretrial briefing or otherwise concludes that further briefing is unnecessary." (Emphasis added.)

Basis for Standing

1. The evidence at issue here consists of Mr. Koerber's private electronic computer files. Alternatively, the evidence at issue consists of private business files over which Mr. Koerber has a reasonable expectation of privacy as effectively the majority owner and the actual controlling manager and/or principal of all related business entities.[1]

2. The files were obtained by the government, without a warrant, from two of Mr. Koerber's former employees. *See* Doc. 411 at 3; *see also* Koerber I, ECF No. 95, at 1, 2-4; *see also* Day 6, Trial Transcript at 1043-1044.

3. The first employee worked for Mr. Koerber as his personal secretary, as a human resources assistant, and as an assistant data entry bookkeeper.

4. The second employee was employed by Mr. Koerber as Mr. Koerber's primary bookkeeper.

5. The copies of the electronic computer files at issue were made from computers controlled and provided by Mr. Koerber and were made by the employees without the knowledge or

[1] It is central to the government's theory of its case that the companies involved in the present indictment were "Mr. Koerber's entities" (*See* Day 6, Trial Transcript at 1043 lines 2-3); and that Mr. Koerber was "in charge" of Franklin Squires (*See* Day 7, Trial Transcript at 1117 lines 10-17), Founders Capital (*id.*), and the other relevant business entities at issue in this motion. *See* Day 26, Trial Transcript at 4763 line 12; *see also* Day 1 Transcript at 6 "[Mr. Koerber] controlled all of those entities. He was in control."

permission of Mr. Koerber, and despite written policy administered by Mr. Koerber, forbidding the copying or private possession of such data.

6. According to the government, both employees made copies of Mr. Koerber's computer files after their bookkeeping responsibilities had ended.

7. According to the government, neither employee searched the files after making copies and removing them from their place of work.

8. The electronic files copied were originally on computers that were provided by Mr. Koerber to the employees to do their work, and the computers and the surrounding work area were under the direct management, supervision and overriding control of Mr. Koerber.

9. Mr. Koerber was the direct supervisor and ultimate boss and authority for both employees during their employment.

10. Mr. Koerber was also the controlling manager, partner, or owner of all of the business entities related to the work done, and the purposes for which each of these files existed on the computers accessed by the employees.

11. The electronic files at issue were created, edited, kept, managed and maintained under the direction of Mr. Koerber, for Mr. Koerber's purposes, and at the time of the government's seizure and subsequent searches only Mr. Koerber had authority or apparent authority to share the files or their contents. Prior to the time of the government's seizures and searches, the records were private, and Mr. Koerber had only authorized these two particular employees to access or search the files in the course of their ministerial duties. *See* Day 7 Trial Transcript at 1246 line 18 to 1247 line 9.

12. As part of their employment by Mr. Koerber, like all other employees, each signed a policy document explaining that the information and files they had access to were private and

confidential, were not the property of company employees and could not be shared or removed without authorization.

13. Under Mr. Koerber's direction, the employees were given workplaces in a secure location within the Franklin Squires building, where Mr. Koerber ensured that electronic key card access was required 24 x7, and where the computers at issue could only be accessed by Mr. Koerber and these employees, using a username and password setup by computer technicians hired and supervised by Mr. Koerber.

14. All of the QuickBooks files described and specified below were individually password protected, with a unique username and password for each file. More specifically, the passwords were created, implemented and authorized by Mr. Koerber (e.g. the main password was the name of one of Mr. Koerber's minor children).

15. Mr. Koerber did not authorize the disclosure of the contents of the private computer files at issue, and no sharing or access of information was allowed without Mr. Koerber's authorization. *See* Day 7 Trial Transcript at 1246 line 18 to 1247 line 9.

16. Mr. Koerber did not authorize the sharing of username or password information for the computers or the files at issue.

17. Mr. Koerber, by virtue of his position as an owner, chief executive, and manager of the employees and information at issue, reasonably expected that these files would not be touched, reviewed or searched by anyone without his permission.

18. Mr. Koerber, and his attorneys, had previously received subpoenas from the IRS requesting all business records and files, which would have included the files at issue here, and Mr. Koerber, through his attorneys, declined to produce and refused to voluntarily provide the

files (including the files at issue here) believing that the subpoenas were, among other things, overbroad and therefore legally ineffective.

19. To resolve this disagreement, the government and Mr. Koerber agreed that the IRS narrowed the scope of the subpoenas to include only paper documents (allowing Mr. Koerber to withhold all electronic files), and to screen for otherwise privileged materials. Thus, Mr. Koerber (through counsel) continued to refuse to disclose voluntarily the electronic files at issue in this motion. *See* Koerber I, May 3, 2010 Hearing Transcript at pp. 15-16, 35-37, 46, 137; *See also* Day 6, Trial Transcript at 1089, 1094.

20. One of the federal agents involved in overseeing the subpoenas and Mr. Koerber's response in 2007, was IRS Agent Marker, who was directly aware of Mr. Koerber's refusal to provide electronic files and the agreement and compromise reached among Mr. Koerber's attorneys and the government, that only paper documents would be produced.

21. Despite the agreement between Mr. Koerber (via counsel) and the government to produce only paper files in response to the 2007 summonses, IRS Agent Marker issued an additional summons to one of the employees and demanded that he produce records (which would have included the records at issue in this motion) under penalty of law. Mr. Koerber (through counsel) intervened, and again refused to voluntarily produce any more than the paper files that had been agreed to, and therefore refused to produce the electronic computer files at issue here.

22. Before the government seized/obtained the computer files from the employees, and prior to any government search of the files, the government had been informed the computer files were Mr. Koerber's and/or that they were under the right and control of Mr. Koerber, and that they had been removed from Mr. Koerber's computers without his permission or knowledge.

23. After the government obtained the computer files on USB drives and/or discs from the employees, the government could not access the QuickBooks files without a username and password for each file. Without a warrant, and without any advance notice to Mr. Koerber or his legal counsel, the government re-contacted the employees asked for and subsequently received the user name and password information.

24. At no time prior to its seizure of Mr. Koerber's computer files did the government inform Mr. Koerber directly or through counsel that it was seeking or intending to seize his private computer files.

25. At no time prior to its seizure did the government seek for or obtain permission from Mr. Koerber to obtain the files, nor did the government seek permission to obtain the confidential passwords.

26. At no time prior to its searches of the computer files, did the government seek or obtain a warrant to seize or search the computer files.

27. At no time prior to its search of the seized computer files did the government inform Mr. Koerber directly or through counsel, that it had possession of his private computer files.

28. At no time prior to searching the files did the government obtain permission or authorization from Mr. Koerber to search the files.

The Evidence for Which Suppression is Sought

Mr. Koerber seeks the return of, and suppression of his personal computer files and/or personal business records provided to the government by his employees. The suppression should also include all fruits derived from these files, including print outs, PDFs and work product derived from access and use of the computer files at issue.

Among these files are what the government previously marked in the last trial as Gov't Exhibits 19, 20, 22, 23, and 24. This also includes the entire contents of the disc and/or hard drives provided by the employees, including but not limited to what the government previously designated as Disc 30 in Koerber I; and the contents of the disc produced by one of the employees in March 2008.

The evidence also includes all username and password protected QuickBooks Files of Mr. Koerber and his companies, including those labeled as Disc 40, Disc 41 and Disc 42, originally produced by the government in Koerber I.

Overview of the Legal Argument

Repeatedly, over the last several years, the United States Supreme Court has reversed trial court rulings or supported the reversal of trial court rulings related to warrantless searches, consistently reminding that, "the Government must generally obtain a warrant supported by probable cause before acquiring such records" particularly related to digital records and modern technology, and that while the "ultimate measure of the constitutionality of a governmental search [or seizure] is reasonableness" in this context, warrantless searches or seizures are typically unreasonable where "undertaken by law enforcement officials to discover evidence of criminal wrongdoing" and in those cases, the government has a burden of showing "a specific exception to the warrant requirement." *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018) (internal quotations and citations omitted). *See also City of Los Angeles, Calif. v. Patel*, 135 S. Ct. 2443, 2448, 192 L. Ed. 2d 435 (2015) (Upholding, among other things, that a hotel's privately kept "business records" where protected from warrantless searches by the Fourth Amendment because the hotel "has the right to exclude others from prying into the[ir] contents."); *Riley v. California*, 134 S. Ct. 2473, 2489, 189 L. Ed. 2d 430 (2014) (Holding that

digital data on cell-phone is especially deserving of Fourth Amendment protections, due in part to the "digital capacity" and broadness of digital "storage capacity" involved and the practical realities of the "digital age[.]"); *United States v. Jones*, 565 U.S. 400, 407 (2012) (Examining and re-affirming the doctrine of *Katz v. United States*, 389 U.S. 347, 351, that without physical trespass, government intrusion (by search or seizure) into a person's private papers or private information generally, is subject to Fourth Amendment protection.)

Here, Mr. Koerber's private computer records are subject to Fourth Amendment protection, and the government's warrantless seizure of these records, and the government's subsequent searching of these records (many of which were password protected) is legally impermissible. Therefore, pursuant to the Fourth Amendment of the United States Constitution, Rules 12(b), 41(g) and 41(h) of the Federal Rules of Criminal Procedure, local rule DUCrimR 12-1(e); and the other legal authority cited below, Mr. Koerber moves to compel the return of his private computer files, and all records and information derived therefrom; Mr. Koerber further moves for an order suppressing these files, and all fruits derived therefrom.

List of the Issues Raised as Grounds for the Motion

In addition to the facts outlined above, Mr. Koerber provides the following list of issues raised as grounds for this motion.

Issue #1: The computer files at issue are Mr. Koerber's personal files. Alternatively, as an owner, controlling office, and manager of Franklin Squires and the related companies at issue here, Mr. Koerber has a legitimate privacy interest in the computer files of Franklin Squires and these companies. *See e.g. City of Los Angeles, Calif. v. Patel*, 135 S. Ct. 2443, 2448, 192 L. Ed. 2d 435 (2015) (Acknowledging that business owners have a Fourth Amendment protected interest in private business records); *New York v. Burger*, 482 U.S. 691, 699 (1987) ("An owner

or operator of a business thus has an expectation of privacy in commercial property, which society is prepared to consider to be reasonable[.]") (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)); *See v. City of Seattle*, 387 U.S. 541, 543 (1967) ("The businessman, like the occupant of a residence, has a constitutional right to go about his business free from unreasonable" searches and seizures under the Fourth Amendment.)

Issue #2: The government knew that employees copied and removed the electronic files at issue, without any apparent or actual authority to do so, prior to requesting that the employees deliver the files to the government. *See e.g. United States v. James*, 353 F.3d 606, 615 (8th Cir. 2003) (Holding that when the government knows prior authority is no longer in place, no legitimate exception based upon apparent authority can be invoked).

Issue #3: The seizure of the files at issue was unreasonable under the Fourth Amendment. *See Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018); *Riley*, 134 S. Ct. at 2495 (holding that records on an electronic storage device (in this case a cell phone) are illegally seized within the meaning of the Fourth Amendment, when those records are otherwise expected to be private under established Fourth Amendment standards.); *Katz*, 389 U.S. 347, 351 ("the Fourth Amendment protects people, not places" and what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.")

Issue #4: According to the government, neither employee searched the files after they were copied and removed from Mr. Koerber's computer (without authorization) nor any other time prior to the files being stored on USB drives and discs later obtained by the government. *See Walter v. United States*, 447 U.S. 649, 657 (1980) ("[T]he Government may not exceed the scope of the private search unless it has the right to make an independent search" and when no

private search has taken place the government's search is "characterized as a separate search" that must be authorized under Fourth Amendment parameters.)

Issue #5: The government's warrantless search of the computer files at issue was unreasonable under the Fourth Amendment. *See e.g. United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (Prior to a search of seized computer files, government "officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations" on a search.); *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982), holding modified by *United States v. Comprehensive Drug Testing, Inc*., 579 F.3d 989 (9th Cir. 2009) ("[T]he wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as the kind of investigatory dragnet that the fourth amendment was designed to prevent.") (Internal quotation omitted.)

Issue #6: The government's warrantless search of the username and password protected QuickBooks files was unreasonable under the Fourth Amendment. *See e.g. United States v. Barrows*, 481 F.3d 1246, 1248 (10th Cir. 2007) (Noting that use of a password significantly effects the evaluation of privacy interests); *see also United States v. Andrus*, 483 F.3d 711, 718 (10th Cir.), decision clarified on denial of reh'g, 499 F.3d 1162 (10th Cir. 2007) (Password-protected files have been compared to a "locked footlocker inside the bedroom." *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir.2001).")

Issue #7: All of the information at issue in this motion was seized and searched by the government as part of direct and deliberate efforts undertaken by law enforcement officials to discover evidence of criminal wrongdoing. Therefore, the government has a burden of showing

"a specific exception to the warrant requirement." *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018).

Mr. Koerber respectfully requests this Honorable Court grant him an evidentiary hearing to establish the facts above and to present argument to the Court. Should the government concede all the facts as described above, Mr. Koerber respectfully urges this Court to grant suppression of the files described herein and any testimony relating thereto and any fruits derived therefrom.

RESPECTFULLY SUBMITTED this 31st day of July, 2018.

/s/ Kathryn N. Nester
Kathryn N. Nester
Federal Public Defender
District of Utah